

HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, Colorado 80527-2400



PATENT APPLICATION

ATTORNEY DOCKET NO. 200205369-1

Inventor(s): Chris D. Hyser

Confirmation No.: 1637

Application No.: 10/693,378

Examiner: Beatrice L.K. Thomas

Filing Date: October 23, 2003

Group Art Unit: 2196

Title: Method and system for distributed key management in a secure boot environment

Mail Stop  
Commissioner For Patents  
PO Box 1450  
Alexandria, VA 22313-1450

**TRANSMITTAL LETTER FOR RESPONSE/AMENDMENT**

Transmitted herewith is/are the following in the above-identified application:

- ☐ Response/Amendment  
☐ New fee as calculated below  
☐ No additional fee  
☒ Other Response to Restriction
- ☐ Petition to extend time to respond  
☐ Supplemental Declaration
- Fee\$ \_\_\_\_\_

CLAIMS AS AMENDED BY OTHER THAN A SMALL ENTITY						
(1) FOR	(2) CLAIMS REMAINING AFTER AMENDMENT	(3) NUMBER EXTRA	(4) HIGHEST NUMBER PREVIOUSLY PAID FOR	(5) PRESENT EXTRA	(6) RATE	(7) ADDITIONAL FEES
TOTAL CLAIMS		MINUS		= 0	X \$50	\$ 0
INDEP. CLAIMS		MINUS		= 0	X \$200	\$ 0
<input type="checkbox"/> FIRST PRESENTATION OF A MULTIPLE DEPENDENT CLAIM					+ \$360	\$ 0
EXTENSION FEE	<input type="checkbox"/> 1st Month \$120	<input type="checkbox"/> 2nd Month \$450	<input type="checkbox"/> 3rd Month \$1020	<input type="checkbox"/> 4th Month \$1590		\$ 0
OTHER FEES						\$
TOTAL ADDITIONAL FEE FOR THIS AMENDMENT						\$ 0

Charge \$ 0 to Deposit Account 08-2025. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450.

Date of Deposit: October 25, 2007

Typed Name: Joanne Bourguignon

Signature: 

Respectfully submitted,

Chris D. Hyser

By 

Robert W. Bergstrom

Attorney/Agent for Applicant(s)

Reg No. : 39,906

Date : October 25, 2007

Telephone : 206.621.1933



PATENT

I hereby certify that on the date specified below, this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Oct. 25, 2007  
Date

Joanne Bourguignon  
Joanne Bourguignon

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Chris D. Hyser  
Application No.: 10/693,378  
Filed: October 23, 2003  
Title: Method and System for Distributed Key Management in a Secure Boot Environment

Examiner: Beatrice L.K. Thomas  
Art Unit: 2196  
Docket No.: 200205369-1  
Date : October 25, 2007

COMMISSIONER FOR PATENTS  
P.O. BOX 1450  
ALEXANDRIA, VA 22313-1450

RESPONSE TO RESTRICTION REQUIREMENT

Sir:

In an Office Communication dated August 15, 2007, the Examiner required restriction of the claims, under 35 U.S.C. § 121 to one of Group I, claims 1-5 and 15-18 and Group II, claims 6-14. Applicant's representative respectfully traverses the restriction requirement, while provisionally electing Group I, claims 1-5 and 15-18.

In justifying the restriction requirement, the Examiner states:

In the instant case, subcombination I has separate utility such as generating an authenticable and verifiable image. Subcombination II has separate utility such as authenticating and verifying an authenticable and verifiable image.

However, this statement is not correct. The method of authenticating and verifying an authenticable and verifiable image, claimed in Group II, requires that the authenticable and verifiable image has been prepared by the method of preparing an authenticable and verifiable image, claimed in Group I. In general, a method for authenticating and verifying electronically encoded information requires that the electronically encoded information contain certain information, that the electronically encoded information was encrypted or otherwise cryptographically protected using a known encryption key or method, or that the

electronically encoded information has been otherwise prepared so that the included information can be extracted and compared with known information, so that the encrypted data can be decrypted, or so that some other forward operation that transforms the information from a first state to a second state can be reversed by applying a backward operation to return the information to the first state. In other words, preparing electronically encoded information for authentication and verification and authenticating and verifying electronically encoded information previously prepared for authentication and verification are quite related operations, generally symmetrical operations or a function/inverse-function pair. In general, unless the method of preparing the electronically encoded information for authentication and verification is an inverse function to the method for authentication and verification of electronically encoded information previously prepared for authentication and verification, or unless both methods are symmetrical, the authentication and verification method will almost certainly fail. For example, if a text file is encrypted using a particular encryption method and key, the encrypted text file can be decrypted only by using a decryption method inverse to the encryption method used to encrypt the text file and a key identical to, or mathematically derived from, the key used for encryption.

In fact, the method of Group II for authenticating and verifying an authenticable and verifiable image fails unless the authenticatable and verifiable image was prepared by the method of Group I. There is no use for the method of Group I unless the method of Group II is employed to subsequently authenticate and verify an authenticatable and verifiable image prepared by the method of Group I. The method of Group II cannot be used unless it is used on an authenticatable and verifiable image prepared by the method of Group I.

The symmetry of the method of Group I and Group II can be easily seen by comparing the elements of claims 1 and 6. Claim 1 recites adding a size and location block, an authentication block including a cryptographically protected module-specific public key and a clear-text version of the module-specific public key to an image, and a verification block that includes a digital signature to an image, while claim 6 recites extracting a module-specific public key and cryptographically protected data related to the module-specific public key from an authenticable and verifiable module, comparing the cryptographically protected data with the module-specific public key, and comparing a value calculated from an image, including a size and location block, to a value extracted from a digital signature contained in a verification block. The operations carried out to authenticate and verify an authenticable and

verifiable image, recited in claim 6, are inverse to the operations carried out to prepare an authenticable and verifiable image, recited in claim 1, and vice versa.

Moreover, according to MPEP § 803:

If the search and examination of an entire application can be made without serious burden, the examiner must examine it on the merits, even though it includes claims to independent or distinct inventions.

As further stated the MPEP § 803:

There are two criteria for a proper requirement for restriction between patentably distinct inventions:

- (A) The inventions must be independent; and
- (B) There must be a serious burden on the examiner if restriction is required. (references to other MPEP sections omitted)

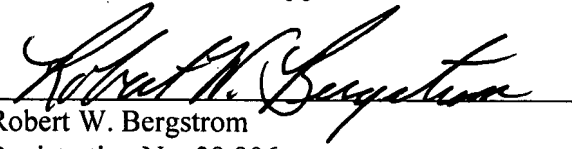
It would be a far more serious burden to redundantly search two entirely related sets of claims than to conduct a single search for both sets of related claims. For example, the various entities added to an image, in the claimed method for preparing an authenticable and verifiable image, are exactly the same entities extracted from an authenticable and verifiable image and used to authenticate and verify the authenticable and verifiable image. Both searches would therefore substantially, if not completely, overlap.

At anytime during the pendency of this application, please charge any fees required or credit any overpayment to Deposit Account No. 08-2025 pursuant to 37 CFR 1.25. Additionally, please charge any fees to Deposit Account No. 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

Chris D. Hyser

OLYMPIC PATENT WORKS <sup>PLLC</sup>

  
Robert W. Bergstrom  
Registration No. 39,906

Enclosure:

Postcards (2)

Transmittal in duplicate

Olympic Patent Works <sup>PLLC</sup>  
P.O. Box 4277  
Seattle, WA 98194-0277